



(19) RU⁽¹¹⁾ 2 007 884⁽¹³⁾ C1
(51) МПК⁵ H 04 L 9/00

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 5012759/09, 22.11.1991

(48) Дата публикации: 15.02.1994

(71) Заявитель:
Березин Борис Владимирович

(72) Изобретатель: Березин Борис Владимирович

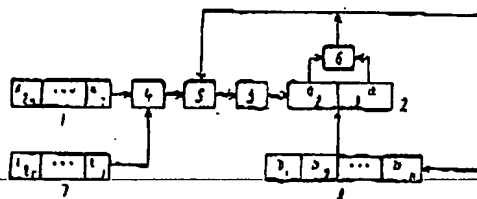
(73) Патентообладатель:
Березин Борис Владимирович

(54) УСТРОЙСТВО ШИФРОВАНИЯ ДВОИЧНОЙ ИНФОРМАЦИИ "АЛБЕР"

(57) Реферат:

Использование: в технике криптографических преобразований в связанных, вычислительных и информационных системах для криптографического закрытия двоичной информации. Сущность изобретения: устройство содержит n-байтный ключевой регистр 1, однобайтный информационный регистр 2, блок 3 функционального преобразования, первый, второй, третий четырехразрядные сумматоры 4 - 6 по модулю два, r-байтный регистр 7, N-битный регистр 8. Обеспечивается возможность реализации устройства на микросхеме, содержащей всего лишь 2 тыс. вентилях, использования ключа такой длины,

которая обеспечивает невозможность его опробования за разумное время. Устройство улучшает криптографические и эксплуатационные параметры устройства шифрования. 2 з. п. ф-лы, 1 ил.



RU 2 007 884 C1

RU 2 007 884 C1

Изобретение относится к криптографическим преобразованиям и может быть использовано в связанных, вычислительных и информационных системах для криптографического закрытия двоичной информации.

Цель изобретения - упрощение аппаратной реализации устройства шифрования до возможности его размещения на микросхеме, содержащей не более 2 тысяч вентилей, а также использование ключа такой длины, которая обеспечивает невозможность его опробования за разумное время.

На чертеже представлена блок-схема предлагаемого устройства.

Устройство шифрования двоичной информации содержит 8-разрядный ключевой регистр 1, 8-разрядный информационный регистр 2, блок 3 четырехразрядный функционального преобразования f , первый, второй, третий четырехразрядные сумматоры 4-6 по модулю два, 8г-разрядный регистр и 7 и N-разрядный регистр 8.

Устройство шифрования двоичной информации работает следующим образом. Выработка полубайта шифрограммы $Ш$ осуществляется следующим образом.

1. В 8-разрядный информационный регистр 2 из N-разрядного регистра 8 записываются восемь бит, например, младших, b_{j1}, \dots, b_{j8} (или два полубайта, $a_2(i), a_1(i)$) исходной информации. Здесь b_{j1}, \dots, b_{jN} - содержимое N-разрядного регистра 8, $b_j = 0, 1, j = 1, N$.

2. Устройство работает пять циклов. Все циклы работы идентичны. В i -й, $1 \leq i \leq 5$ цикл работы к сумме i -го (по модулю $2n$) полубайта ключевого регистра 1 и i -го (по модулю $2r$) полубайта ключевого регистра 7 прибавляется сумма первого и второго полубайтов 8-разрядного информационного регистра 2, полученная схема преобразуется блоком 3 и результат записывается в 8-разрядный информационный регистр 2 на освободившееся место после сдвига его содержимого на один полубайт в сторону младших разрядов (вправо). После i -го цикла содержимое 8-разрядного информационного регистра 2 следующее:

$$a_2(i+1) = f(k_1 \text{ (mod } 2n) +$$

$$+ k_4 \text{ (mod } 2r) + (a_1(i) + a_2(i)),$$

два полубайта 8-разрядного информационного регистра 2 перед началом i -го цикла, $1 \leq i \leq 5$:

$$a_2(i), a_1(i) - \text{исходное состояние регистра 2;}$$

$a_2(s+1), a_1(s+1)$ - результирующее состояние регистра 2.

k_1, \dots, k_{2n} - $2n$ полубайт - n -байтного ключа.

k_1, \dots, k_{2r} - $2r$ полубайт содержимого регистра 2;

$+$ - сложение полубайтов по модулю 2 либо 2^4 .

f - функция 2^4 -значной логики (система 4-двоичных функций от 4-двоичных переменных);

$$a_1(i), a_2(i), k, k_1 \in \{0, 1, \dots, 15\}, i \geq 1.$$

Если выбрать третий четырехразрядный сумматор 6 по модулю 2^4 , а первый и второй четырехразрядные сумматоры 4 и 5 по модулю 2, к ключевому полубайту прибавлять сначала полубайт из регистра 7, а затем уже

сумму полубайта регистра 2, то после i -го цикла содержимое 8-разрядного информационного регистра 2 следующее:

$$a_2(i+1) = f(k_1 \text{ (mod } 2n) \oplus k_4 \text{ (mod } 2r) \oplus (a_1(i) \oplus a_2(i)),$$

$$a_1(i+1) = a_2(i), i \geq 1$$

\oplus - поразрядное сложение полубайтов по модулю 2;

\oplus - сложение полубайтов по модулю 2^4 .

3. Сумма полученных в 8-разрядном информационном регистре 2 после s -го цикла двух полубайт $a_1(s+1), a_2(s+1)$ является полубайтом шифрограммы $Ш$, т. е. $Ш = a_1(s+1) \oplus a_2(s+1)$.

В блоке 3 реализуется функция 2^4 -значной логики, представленная в дизъюнктивной форме системой четырех двоичных функций y_1, \dots, y_4 от четырех двоичных переменных x_1, \dots, x_4 , $y_i, x_i = 0, 1, i = 1, 4$.

В качестве функционального преобразования f можно выбрать, например, следующее:

$$y_1 = x_1x_4 \vee x_1x_2x_4 \vee x_1x_2x_3x_4 \vee x_1x_2x_3x_4$$

$$y_2 = x_2x_3 \vee x_2x_3x_4 \vee x_1x_2x_3x_4 \vee x_1x_2x_3x_4$$

$$y_3 = x_1x_2x_3 \vee x_1x_2x_4 \vee x_1x_2x_3x_4 \vee x_1x_2x_4$$

$$y_4 = x_2x_3x_4 \vee x_1x_2x_3 \vee x_1x_2x_3 \vee x_2x_3x_4$$

Увеличение числа циклов работы устройства шифрования повышает уверенность в криптографической надежности зашифрования информации, т. е. в том, что никому не удастся расшифровать сообщение за время, меньшее чем полное опробование всех возможных вариантов n -байтного ключа. Вместе с тем, чем больше циклов работает устройство для выработки одного полубайта шифрограммы, тем меньше его производительность. Это дает возможность выбора между риском и производительностью. Рекомендуется выбирать число 5 циклов работы устройства шифрования в пределах от $4n$ до $16n$, где n - длина ключа в байтах. Реальная длина ключа - от 8 до 16 байт.

Для выработки следующего полубайта шифрограммы используются 8 бит b_{j1}, \dots, b_{j8} следующего состояния N-разрядного регистра 8.

В качестве N-разрядного регистра 8 можно выбрать 15-разрядный регистр сдвига со следующей линейной функцией максимального периода 2^{15} в обратной связи: $b_{15} = b_1 \oplus b_2$. Если текущее состояние регистра сдвига обозначить через b_1, \dots, b_{15} , где $b_i = 0, 1, i = 1, 15$, то следующее состояние регистра сдвига будет $b_2, \dots, b_{15}, b_1 \oplus b_2$.

В 8г-разрядный регистр 7 записывается представленное в двоичном виде текущее время (месяц, число, час, минуты, секунда) или случайное число, вырабатываемое датчиком случайных чисел. Вместе с временем или случайным числом можно записывать также и номер передзвонящего абонента. Реальная длина регистра 8г - 4-8 байт. Очередное состояние 8г-разрядного регистра 7 используется для выработки 2^{N-1} полубайт шифрограммы $Ш$, после чего в 8г-разрядный регистр 7 записывается новое время или новое случайное число.

При использовании единого времени оно не должно повторяться все время действия ключа. Например, если ключ действует один год, то время должно включать в себя месяц, если ключ действует несколько лет, то также и год.

После установки нового состояния в 8-разрядный регистр 7 устройство шифрования формирует новое начальное состояние N-разрядного регистра 8. В случае 15-разрядного битного двоичного регистра сдвига можно предложить следующую процедуру формирования нового начального состояния.

Устройство шифрования прокручивается 5 циклов, как это было описано. Полученные после m-го, 3m-го, 5m-го, 7m-го циклов, где m это целая часть числа $8^{-1} s$, 4 полубайта

$$a_2(m+1) + a_1(m+1),$$

$$a_2(3m+1) + a_1(3m+1),$$

$$a_2(5m+1) + a_1(5m+1),$$

$a_2(7m+1) + a_1(7m+1)$ записываются в регистр 8. В старшие два бита полубайта $a_2(7m+1) + a_1(7m+1)$ принудительно записываются нули 1. Так как в выбранном регистре 8 всего 15 разрядов, то четвертый бит последнего полубайта не используется.

Очередное состояние 8-разрядного регистра 7 и новое исходное состояние 15-разрядного двоичного регистра 8 сдвига используются для выработки 2^{14} -полубайт (-2^{18} бит) шифрграммы, после чего требуется обновление состояния регистров 7 и 8.

Шифрграмма Ш складывается по модулю 2 с представленным в двоичном виде открытым сообщением А. Полученное зашифрованное сообщение В = А ⊕ Ш вместе с заполнением 8-разрядного регистра 7 передается получателю.

Принимающий абонент устанавливает в 8-разрядный регистр 7 своего устройства шифрования принятые г-байт и вырабатывает описанным способом шифрграмму Ш. Затем принимающий абонент складывает ее по модулю 2 с принятым зашифрованным сообщением В и получает открытое сообщение А = В ⊕ Ш. (58) Сяо Д., Керр Д.

и Мэдник С. Защита ЭВМ. М.: Мир, 1982, с. 137-162.

Формула изобретения:

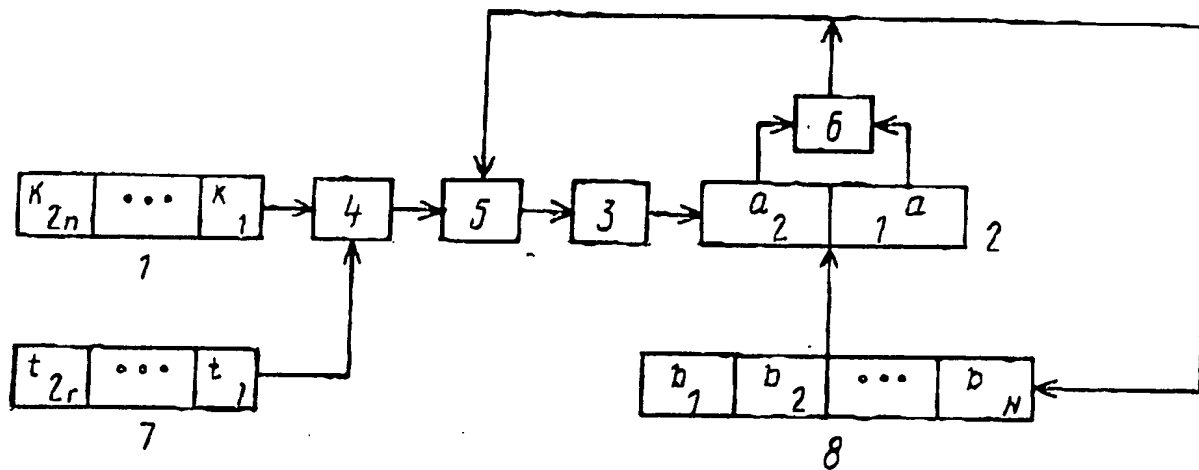
1. Устройство шифрования двоичной информации, содержащее ключевой регистр и последовательно соединенные блок многоразрядного функционального преобразования f и информационный регистр, отличающееся тем, что в нем ключевой регистр выполнен в виде n-разрядного ключевого регистра, информационный регистр выполнен в виде 8-разрядного информационного регистра, блок многоразрядного функционального преобразования f выполнен в виде блока 4-разрядного функционального преобразования, при этом в него введены первый, второй и третий 4-разрядных сумматора и i-разрядный регистр, причем выход ключевого регистра подключен к первому входу первого сумматора, выход которого подключен к первому входу второго сумматора, выход второго сумматора подключен к входу блока 4-разрядного функционального преобразования f, выход которого подключен к второму четырехразрядному входу информационного регистра, оба четырехразрядных выхода которого подключены к двум входам третьего сумматора, выход третьего сумматора подключен к второму входу первого сумматора, если i-разрядный регистр подключен к второму входу второго сумматора, или к второму входу второго сумматора, если i-разрядный регистр подключен к второму входу первого сумматора.

2. Устройство по п. 1, отличающееся тем, что в него дополнительно введен N-разрядный регистр, причем 8-разрядный выход N-разрядного регистра подключен к входу 8-разрядного информационного регистра.

3. Устройство по п. 1, отличающееся тем, что вход N-разрядного регистра подключен к выходу третьего четырехразрядного сумматора.

RU 2007884 C1

RU 2007884 C1



RU 2007884 C1

RU 2007884 C1

DEVICE FOR ENCRYPTING BINARY INFORMATION

Patent Number: RU2007884
Publication date: 1994-02-15
Inventor(s): BEREZIN BORIS V (RU)
Applicant(s): BEREZIN BORIS V (RU)
Requested Patent: ☐ RU2007884
Application Number: SU19915012759 19911122
Priority Number(s): SU19915012759 19911122
IPC Classification: H04L9/00
EC Classification:
Equivalents:

Abstract

Data supplied from the **esp@cenet** database - I2

Dr. Mikhail Gorodissky (1927-2002)
 Dip. Eng. Valery Mordvedov, PA, EPA, TMA
 Dr. Econ. Anatoly Pavlovsky, PA, EPA
 Dip. Eng. Gergey Dudushkin, PA, EPA, TMA, DA
 Dip. Econ. Anatoly Shalikhov, TMA
 Dip. Eng. Natalia Lebedeva, PA, EPA
 Dip. Eng. Elena Tomskaya, PA, EPA
 Dip. Law. Vladimir Birtulin, L, PA
 Dip. Eng. Yuri Kuznetsov, PA, EPA, TMA, L
 Dip. Ling. Galina Egorova, PA
 Dip. Ling. Ludmila Kiriushina, PA, EPA, TMA, DA
 Dip. Eng. Alexander Vasillets, DA, PA, TMA
 Dip. Chem. Elena Nazina, PA, EPA
 Dip. Ling. Irina Korzun, TMA
 Dip. Eng. Sergey Dorofeev, PA, EPA, TMA
 Dip. Eng. Evgeny Emeftanov, PA, EPA
 Dip. Eng. Vladimir Mescheriakov
 Dip. Eng. Alexander Mirts, PA

Dip. Eng. Valery Kallnovsky*, TMA, PA
 Dip. Law. Igor Rabkovsky*, L, PA, TMA



GORODISSKY & PARTNERS

Since 1959

S. 04/14
 TRADEMARKS
 DESIGNS
 COPYRIGHT
 LICENSING
 LITIGATION

St. Petersburg

Dip. Eng. Viktor Stankovsky, PA, TMA, DA
 Dip. Eng. Valeria Nazarova, TMA
 Dip. Eng. Natalia Potanina, PA
 Dip. Eng. Elena Chugorina, DA
 Dip. Law. Maria Nosova, L

N. Novgorod

Dip. Eng. Irina Shishko
 Dip. Chem. Ludmila Pozina

Krasnodar

Dip. Eng. Tatiana Titova
 Dip. Law. Vadim Bloshentsev, L

Samara

Dip. Ling. Galina Skrebkova
 Dip. Law. Nadezhda Zagumennikova, L

Ekaterinburg

Dip. Eng. Sergey Egorov
 Dip. Eng. Nina Andreeva, PA
 Dip. Eng. Ekaterina Glebova

Kiev (Ukraine)

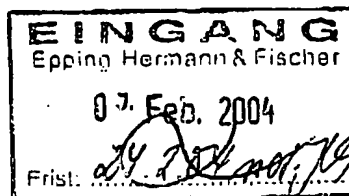
Dip. Eng. Nina Moshinskaya, L, PA, TMA, DA
 Dip. Ling. Sergey Novikov, L, PA, TMA, DA
 Dip. Ling. Yuliya Grabovska, L, TMA, DA, PA
 Dip. Eng. Natalia Breus, L, PA, DA, TMA

Moscow
 St. Petersburg
 N. Novgorod
 Krasnodar
 Samara
 Ekaterinburg
 Kiev (Ukraine)

PA - Patent Attorney
 EPA - Eurasian Patent Attorney
 TMA - Trademark Attorney

DA - Design Attorney
 L - Lawyer
 * - Consultant

Epping - Hermann - Fischer
Patentanwalts-gesellschaft mbH
POSTFACH 12 10 26
80034 MUENCHEN
DEUTSCHLAND
PCT/DE99/00278



VIA DHL

Date: 06 February 2004

Your Ref: 1998P1180PRU(EG)
Our Ref: 2412-222340/1152
Country: RUSSIA
Appl No: 2000123792
Pat No:

In the name of:
INFINEON TECHNOLOGIES AG

JOS P. U.S.A F: 14.3.04 mof

Dear Sirs,

We are glad to announce that an Official Decision of Grant has been issued in respect of the above application and received from the Patent Office of the Russian Federation on **14 January 2004**. Please be informed that in accordance with the current Russian Patent Law which came into force on March 12, 2003 the payment of Grant and Renewal fees should be effected within two months from above date, that is not later than **14 March 2004**.

The Grant fee amounts to **400 US\$**, our fee is **200 US\$**. The Renewal fees payable from the third year of patent duration should be paid for the period from **02 February 2001** till **02 February 2005** in the amount of **500 US\$**, our fee is **260 US\$**.

Please bear in mind that if the fees are not paid before the above date the payment in question is possible within six months from said date but with a fine of 50%.

We look forward to your consent to payment of the fees by **29 February 2004**.

*F. JS CP 1.001
 10.02.04*

Yours sincerely,

Yury D. Kuznetsov
Patent Attorney
Chief of electronics and
physics department

Encl.: [x] Decision of Grant
[x] Comments

[x] Invoice

Client's code - DE92433

Address:
 Law firm "Gorodissky & Partners" Ltd.
 B. Spasskaya str., 25, stroenie 3
 Moscow 129010, Russia

Telephone:
 +7 (095) 937 6118 / 6109

Fax:
 +7 (095) 937 6104 / 6123

Internet:
 E-mail: pat@gorodissky.ru
<http://www.gorodissky.com>



РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ
(РОСПАТЕНТ)

☑ (74)

ОТДЕЛ И 9

**ФЕДЕРАЛЬНЫЙ ИНСТИТУТ
ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ**

Бережковская наб., 30, корп. 1, Москва, Г-59, ГСП-5, 123995
Телефон 240 60 15. Телекс 114818 ПДЧ. Факс 243 33 37

На № 2412-222340/1152 от 15.07.2003

129010, Москва, ул. Б. Спасская, 25, стр. 3,
ООО "Юридическая фирма Городисский и
Партнеры", пат. пов. Ю.Д.Кузнецову, рег.№
595

(21) Наш № 2000123792/09(025709)

При переписке просим ссылаться на номер заявки и
сообщить дату получения данной корреспонденции

РЕШЕНИЕ О ВЫДАЧЕ

ПАТЕНТА НА ИЗОБРЕТЕНИЕ

(21) Заявка № 2000123792/09(025709)

(22) Дата подачи заявки 02.02.1999

✓ (24) Дата начала отсчета срока действия патента 02.02.1999

(85) Дата начала рассмотрения международной заявки на национальной фазе 18.09.2000

ПРИОРИТЕТ УСТАНОВЛЕН ПО ДАТЕ

☐ (22) подачи заявки

☐ (23) поступления дополнительных материалов от
к ранее поданной заявке № от

☐ (62) ☐ приоритета изобретения по первоначальной заявке № от
из которой данная заявка выделена

☐ подачи первоначальной заявки № от
из которой данная заявка выделена

☐ (66) подачи ранее поданной заявки № от

☑ (30) подачи первой заявки в государстве-участнике Парижской конвенции

(31) Номер первой (ых)
заявки(ок)

(32) Дата подачи первой(ых)
заявки(ок)

(33) Код страны

Пункт
формулы

✓ 1. 19806825.5 ✓
2.
3.

18.02.1998 ✓

DE

(86) Заявка №РСТ/ DE99/00278 от 02.02.1999

(96) Заявка №ЕА

(87) Номер публикации и дата публикации заявки РСТ WO 99/43124, 26.03.1999

(72) Автор(ы) ХЕСС, Эрвин, ГЕОРГИАДЕС, Жан, DE

(73) Патентообладатель(и) ИНФИНЕОН ТЕКНОЛОДЖИЗ АГ, DE

(указать код страны)

(51) МПК 7 H04 L 9/30

(54) Название изобретения Способ криптографической обработки с использованием эллиптической кривой с помощью вычислительного устройства и устройство для осуществления способа

02 2

ДОМ 15.07.2003

091801

(21) 2000123792/09

(54) (57)

1. Способ оптимального использования области памяти на портативном носителе информации, предназначенной для хранения параметров эллиптических кривых, причем параметры предназначены для криптографической обработки с помощью эллиптической кривой с использованием вычислительного устройства, при котором а) задают эллиптическую кривую первой формы, причем эллиптическую кривую определяют несколько первых параметров, б) преобразуют эллиптическую кривую во вторую форму

$$y^2 = x^3 + c^4 ax + c^6 b$$

путем определения нескольких вторых параметров, причем по меньшей мере один из вторых параметров сокращен по своей длине по сравнению с первым параметром, где x, y – переменные,

a, b – первые параметры и c – константа,

в) причем по меньшей мере сокращают параметр a путем выбора константы c так, что выражение $c^4 a \bmod p$ определяется с существенно меньшей длиной по сравнению с длиной параметра b и длиной заданной величины p , г) и при этом эллиптическую кривую второй формы сохраняют на носителе информации и используют в криптографической обработке.

2. Способ по п.1, отличающийся тем, что первая форма эллиптической кривой определяется выражением $y^2 = x^3 + ax + b$, где x, y – переменные, a, b – первые параметры.

3. Способ по п.1 или п.2, отличающийся тем, что осуществляют криптографическое кодирование.

4. Способ по любому из пунктов 1-3, отличающийся тем, что

осуществляют криптографическое декодирование.

5. Способ по любому из пунктов 1-4, отличающийся тем, что осуществляют присвоение кода.

6. Способ по любому из пунктов 1-5, отличающийся тем, что осуществляют цифровую подпись.

7. Способ по п.6, отличающийся тем, что осуществляют проверку цифровой подписи.

8. Способ по любому из пунктов 1-7, отличающийся тем, что осуществляют асимметричную аутентификацию.

9. Карточка со встроенной микросхемой для криптографической обработки с использованием эллиптической кривой, содержащая область памяти, предназначенную для сохранения параметров эллиптической кривой, и процессорный блок, который выполнен так, что а) задается эллиптическая кривая первой формы, причем эллиптическая кривая определяется несколькими параметрами, б) обеспечивается возможность преобразования эллиптической кривой во вторую форму $y^2 = x^3 + c^4 ax + c^6 b$ путем определения нескольких вторых параметров, причем по меньшей мере один из вторых параметров по своей длине сокращается по сравнению с первым параметром, где x, y – переменные, a, b – первые параметры и c – константа,

в) причем по меньшей мере сокращается параметр a путем выбора константы c так, что выражение $c^4 a \bmod p$ определяется с существенно меньшей длиной по сравнению с длиной параметра b и длиной заданной величины p , г) и при этом эллиптическую кривую второй формы сохраняют на носителе информации и используют в криптографической обработке.

10. Карточка со встроенной микросхемой по п.9, отличающаяся тем, что в защищенной области памяти карточки со встроенной микросхемой хранится секретный код.

US5442707A, 15.08.1995 aus WO bekannt

SU 1349685 A, 30.05.1987 ✓ CPl & Schreiben v. 25.02.04 falsch, richtig: RU 2007 884
29.02.04
JC

При публикации сведений о выдаче патента описание будет
использовано в первоначальной редакции заявителя

При публикации сведений о выдаче патента будут использованы
первоначальные чертежи.

Приложения: 1 Реферат, скорректированный экспертизой, на 1л. в 1
экз.

Главный государственный патентный
эксперт отдела электрорадиотехники
Сурина 240 35 76



А.Б.Михайлова

Приложение к решению о выдаче патента на изобретение по заявке
№2000123792/09(025709) на 1 л. в 1 экз.

К заявке №2000123792/09

МПК 7 H04 L9/30

(54) Способ криптографической обработки с использованием эллиптической кривой с помощью вычислительного устройства и устройство для осуществления способа

Реферат

(57) Изобретение относится к криптографии. Технический результат заключается в уменьшение длины по меньшей мере одного параметра эллиптической кривой и обеспечения высокой надежности. Для этого параметры эллиптической кривой хранят в запоминающем устройстве вычислительного устройства. Эти параметры имеют значительную длину. С помощью определенного алгоритма параметр сокращают, тогда как другие параметры составляют длину, равную нескольким сотням битов. 2 н.п., 8 з.п. ф-лы, 5ил, 8 табл.

Референт

Е.Я.Сурина



G O R O D I S S K Y & P A R T N E R S

Since 1959

DESIGNS
COPYRIGHT
LICENSING
LITIGATION

Dr. Mikhail Gorodissky (1927-2002)
Dip. Eng. Valery Medvedev, PA, EPA, TMA
Dr. Econ. Anatoly Pavlovsky, PA, EPA
Dip. Eng. Sergey Duduchkin, PA, EPA, TMA, DA
Dip. Econ. Anatoly Shalikhov, TMA
Dip. Eng. Natalia Lebedeva, PA, EPA
Dip. Eng. Elena Tomskaya, PA, EPA
Dip. Law. Vladimir Birluin, L, PA
Dip. Eng. Yuri Kuznetsov, PA, EPA, TMA, L
Dip. Ling. Galina Egorova, PA
Dip. Ling. Ludmila Kriushina, PA, EPA, TMA, DA
Dip. Eng. Alexander Vasilev, DA, PA, TMA
Dip. Chem. Elena Nazina, PA, EPA
Dip. Ling. Irina Korzun, TMA
Dip. Eng. Sergey Dorofeev, PA, EPA, TMA
Dip. Eng. Evgeny Emelev, PA, EPA
Dip. Eng. Vladimir Mascheriakov
Dip. Eng. Alexander Mits, PA

St. Petersburg

Dip. Eng. Viktor Stanovsky, PA, TMA, DA
Dip. Eng. Valeria Nazarova, TMA
Dip. Eng. Natalia Patanina, PA
Dip. Eng. Elena Chugorina, DA
Dip. Law. Maria Nosova, L

N. Novgorod

Dip. Eng. Irina Shishko
Dip. Chem. Ludmila Pazina

Krasnodar

Dip. Eng. Tatiana Titova
Dip. Law. Vadim Blashentsev, L

Samara

Dip. Ling. Galina Skrebkova
Dip. Law. Nadezhda Zagumennikova, L

Ekaterinburg

Dip. Eng. Sergey Egorov
Dip. Eng. Nina Androeva, PA
Dip. Eng. Ekaterina Glebova

Kiev (Ukraine)

Dip. Eng. Nina Mashinskaya, L, PA, TMA, DA
Dip. Ling. Sergey Novikov, L, PA, TMA, DA
Dip. Ling. Yuliya Grabovska, L, TMA, DA, PA
Dip. Eng. Natalia Breus, L, PA, DA, TMA

Est. 1959
Moscow
St. Petersburg
N. Novgorod
Krasnodar
Samara
Ekaterinburg
Kiev (Ukraine)

Dip. Eng. Valery Kalinovsky*, TMA, PA
Dip. Law. Igor Rabkovsky*, L, PA, TMA

Epping - Hermann - Fischer
Patentanwalts-gesellschaft mbH
POSTFACH 12 10 26
80034 MUENCHEN
DEUTSCHLAND
PCT/DE99/00278

14.03.2004 = 225
Per. net.

PA - Patent Attorney
EPA - Eurasian Patent Attorney
TMA - Trademark Attorney

DA - Design Attorney
L - Lawyer
- Consultant

Date: 25 February 2004

YourRef: 1998P1180PRU(EG)
OurRef: 2412-222340/1152
Country: RUSSIA
ApplNo: 2000123792
PatNo:

In the name of:
INFINEON TECHNOLOGIES AG

Dear Sirs,

We acknowledge your instructions of 17 February 2004 to pay the grant and renewal fees on the above case which will be effected in time by Mrs. L. Kiriushina, Chief of annuities payment department.

As our involvement in this application has now concluded we take this opportunity to thank you for your cooperation and would be always at your disposal if some questions concerning essence of invention may arise in future.

All questions concerning annuities or obtaining Letters Patent please address directly to Mrs. L. Kiriushina, using her reference number 2410-222340.

As to the cited reference SU 1349685 A, please be advised that it was indicated in the Official Decision of Grant by mistake. Instead of it we enclose herewith a copy of reference RU 2 007.884.C1, 15.02.1994, which is a correct one.
We offer you our sincere apologies for this mistake.

Yours sincerely,

Yuri D. Kuznetsov
Patent Attorney
Chief of electronics and
physics department
Encl.

Client's code - DE92433

Address:
Law firm "Gorodissky & Partners" Ltd.
B. Spasskaya str., 25, entrance 3
Moscow 125010, Russia

Telephone:
+7 (095) 937 6116 / 6109

Fax:
+7 (095) 937 6104 / 6123

Internet:
E-mail: p31@gorodissky.ru
http://www.gorodissky.com

